FINITE FIELDS AND THEIR APPLICATIONS **2,** 321–335 (1996)
ARTICLE NO. 0020

The Incongruence of Consecutive Values of Polynomials

PIETER MOREE*

School of MPCE, Macquarie University, Sydney, New South Wales 2109 Australia
E-mail: moree@antigone.mpim-bonn.mpg.de; moree@rulfc1.leidenuniv.nl

Communicated by Gerhard Turnwald

Received January 19, 1995; revised March 4, 1996

Suppose that $f \in \mathbb{Z}|x|$. Put $D_f(n) = \min\{k > 0 \mid f(1), \ldots, f(n)$ are pairwise incongruent modulo $k\}$. Special cases of this function were previously considered, using methods from elementary number theory. Results from the theory of finite fields are used to prove a theorem that for all f in a large subset of $\mathbb{Z}|x|$ provides a characterization of $D_f(n)$ for all n sufficiently large. This theorem partially encompasses results due to Bremser, Schumer and Washington and to Moree and Mullen, who characterized $D_f(n)$ for cyclic, respectively, Dickson polynomials.

1. INTRODUCTION

Suppose that $f \in \mathbb{Z}|x|$. For an arbitrary positive integer n, let $D_f(n)$ denote the smallest positive integer k such that $f(1), \ldots, f(n)$ are pairwise distinct modulo k. In case this number does not exist, we put $D_f(n) = \infty$. In this paper we will consider the problem of characterizing the function D_f for a given polynomial f. Throughout the paper we assume that $\deg f > 1$. Whenever $D_f(n) = \infty$ for some n, this characterization reduces to a finite problem and so one might as well restrict oneself to those f that act injectively on $\mathbb{N}$. Arnold *et al.* [1] were the first to consider $D_f(n)$ for some f. They considered $D_{x^2}(n)$, baptized it discriminator, and used this function in developing an algorithm to quickly calculate square roots of a long sequence of integers. The next case considered was $f = x^j$ for arbitrary j with $D_{x^j}(n)$ denoted by $D(j, n)$. Schumer [13] considered the cases where

* Present address: Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, 53225 Bonn, Germany.

1071-5797/96 $18.00

$j = 3$ and 6, and in [14], Schumer and Steinig considered the case $j = 2^h$ for $h \geq 2$. Barcau [2] resolved the case where j is an odd prime. The main result in the case f is a cyclic polynomial is due to Bremser *et al.* [3]. It gives an asymptotic characterization, that is, characterization for all n sufficiently large, of $D(j, n)$ and for j is odd is reproduced in Theorem 1. In the statement of Theorem 1, as in the rest of this paper, the letter p is used to denote a prime. Furthermore $\varphi(k)$ denotes Euler's totient and (a, b) denotes the greatest common divisor of a and b.

THEOREM 1. *Let $j \geq 3$ be odd and let B_j be the smallest integer such that for all $n \geq B_j$, there exists a prime p with $(p - 1, j) = 1$ and $n \leq p < 4n/3$. Then for $n \geq B_j$,*

$$D(j, n) = \min\{k \geq n \mid (j, \varphi(k)) = 1 \text{ and } k \text{ is squarefree}\}.$$

By the Prime Number Theorem for arithmetic progressions (see, for example, [5, Chaps. 20 and 22]) there is always a prime $p \equiv 2 \pmod{j}$ in $[n, 4n/3)$ for n sufficiently large, and so B_j exists. Moree and Mullen [10] considered $D_f(n)$ with f a Dickson polynomial. The Dickson polynomial of degree $j \geq 1$ and parameter $a \in \mathbb{Z}$ is defined by

$$g_j(x, a) = \sum_{i=0}^{[j/2]} \frac{j}{j-i} \binom{j-i}{i} (-a)^i x^{j-2i},$$

where $[\cdot]$ denotes the greatest integer function. It can be shown that $g_j(x, a) \in \mathbb{Z}[x]$. Notice that $g_j(x, 0) = x^j$. In what follows we will reserve the term Dickson polynomial for polynomials $g_j(x, a)$ with $a \neq 0$. For a wealth of further material on Dickson polynomials, the reader is referred to [7]. Moree and Mullen [10, Theorem 9] gave the following asymptotic characterization of $D_{g_j(x,a)}(n)$:

THEOREM 2. *Let $a \in \mathbb{Z}$. Put $\psi_a(k) = \varphi(k) \prod_{p \mid k, p \nmid a} (p + 1)$ and define the a-part of k to be the largest divisor of k having only prime factors dividing a. Let $j \geq 3$ be odd and if $a \neq 0$ suppose that furthermore $3 \nmid j$. Let E_j be the smallest integer such that for all $n \geq E_j$ there exists an integer k having squarefree a-part with $(j, \psi_a(k)) = 1$ and $n \leq k \leq 2n - 3$. Then, for every $n \geq E_j$,*

$$D_{g_j(x,a)}(n) = \min\{k \geq n \mid (j, \psi_a(k)) = 1 \text{ and the a-part of } k \text{ is squarefree}\}.$$

The existence of E_j is guaranteed by the Prime Number Theorem for arithmetic progressions. Notice that Theorem 2 strengthens Theorem 1. In

the case $6 \nmid a$ it can even be shown that the conclusion of Theorem 2 is valid for all $n \geq 1$ [10, Theorem 9 (iii)].

Let R be a finite commutative ring. A polynomial $f \in R[x]$ is said to be a permutation polynomial of R if it permutes the elements of R under the evaluation mapping. It is known [10, Lemma 11 (iii)] that for $j > 1$, $g_j(x, a)$ permutes $\mathbb{Z}/k\mathbb{Z}$ if and only if $(j, \psi_a(k)) = 1$ and the a-part of k is squarefree. Thus Theorem 2 gives a characterization of the form $D_f(n) = \min\{k \geq n \mid f \text{ permutes } \mathbb{Z}/k\mathbb{Z}\}$, with f a Dickson polynomial or cyclic polynomial. The question that arises is to find necessary and sufficient conditions for f to have an asymptotic characterization of the above form. The main result of this paper gives an asymptotic characterization of $D_f(n)$ for a large set of $f \in \mathbb{Z}[x]$ including cyclic and Dickson polynomials. Before stating the result we give some notation. Put $V_f(k) = |\{f(a) \mid a \in \mathbb{Z}/k\mathbb{Z}\}|$. Thus, $V_f(k)$ is the cardinality of the value set of f over $\mathbb{Z}/k\mathbb{Z}$. Put $S(f) = \sup\{V_f(p)/p \mid V_f(p) < p\}$ and $C(f) = \max\{2/3, S(f)\}$. For given $\mu > 1$ and f let n_μ denote the smallest integer ≥ 4 such that $[n, \mu n]$ contains at least one integer k such that f permutes $\mathbb{Z}/k\mathbb{Z}$ for every $n \geq n_\mu$ if it exists. Denote $n_{1/C(f)}$ by $n(f)$ if it exists.

THEOREM 3. *Suppose that $n(f)$ exists. Then, for every $n \geq n(f)$,*

$$D_f(n) = \min\{k \geq n \mid f \text{ permutes } \mathbb{Z}/k\mathbb{Z}\}.$$

In Section 2 a proof of Theorem 3 will be given. Here we will content ourselves with a discussion of the key idea.

For convenience put $K_f = \{k \geq 1 \mid f \text{ permutes } \mathbb{Z}/k\mathbb{Z}\}$ and $M_f(n) = \min\{k \geq n \mid k \in K_f\}$. The polynomials x^j and $g_j(x, a)$ with j odd and in the latter case j not divisible by 3 are special in that they permute $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p. By the Chinese Remainder Theorem it then follows that there are "many" integers in K_f ("many" is specified in Section 4 of [10]). The consequences of this are twofold. First, any integer $k \geq n$ that is in K_f yields an upper bound for $D_f(n)$. In particular $D_f(n) \leq M_f(n)$. Proving the reverse inequality is the difficult part in establishing Theorems 1 and 2. For this it turns out to be essential that $M_f(n)/n$ is sufficiently close to 1. That this is indeed the case is the second consequence of the ubiquity of the integers k such that f permutes $\mathbb{Z}/k\mathbb{Z}$. A little finite field theory leads immediately to an explanation of why one needs $M_f(n)/n$ to be small. Mullen [12] conjectured and Wan [19] proved the following result.

LEMMA 1. *Suppose that f does not permute $\mathbb{Z}/p\mathbb{Z}$ with p a prime. Then*

$$V_f(p) \leq \left[p - \frac{p-1}{d} \right] \leq p\left(1 - \frac{1}{2d}\right),$$

where d denotes the degree of f.

Lemma 1 declares that "near" permutation polynomials do not exist. Wan used p-adic methods to prove this result. Very recently Lenstra (unpublished manuscript) and independently Turnwald [18] found an elementary proof of Wan's result. Lemma 1 trivially extends to squarefree integers; that is, $V_f(k) \leq k(1 - 1/(2d))$, for squarefree k in case f does not permute $\mathbb{Z}/k\mathbb{Z}$. Now suppose that there exists $c < 1$ such that $V_f(k) \leq ck$ for all positive integers k such that f does not permute $\mathbb{Z}/k\mathbb{Z}$. Then, provided that $M_f(n)/n < 1/c$, we must have $D_f(n) = M_f(n)$. A validation of this claim is as follows. Put $k = D_f(n)$. Note that $n \leq k < n/c$. By the definition of the discriminator $V_f(k) \geq n > kc$ and so f must permute $\mathbb{Z}/k\mathbb{Z}$. Using the definition of $M_f(n)$ and $D_f(n) \leq M_f(n)$ it then follows that $D_f(n) = M_f(n)$. This simple argument is at the heart of the proof of Theorem 3. Unfortunately the assumption on V_f is not true for all f. (It can be shown, using Schur's conjecture [6], that it is not true if and only if f can be written as a composition of [linear translates of] Dickson polynomials of odd degree not divisble by 3 and at least one cyclic polynomial of odd degree exceeding 1.) The assumption on V_f, however, is true on restricting oneself to squarefree integers and this turns out to be enough to salvage this approach of proving Theorem 3. The details are in Section 2.

The above discussion makes it clear that the quantity $\gamma(f) := \limsup_{i\to\infty} k_{i+1}/k_i$, where $k_1, k_2, \ldots$ denote the consecutive elements of K_f, plays an important role. The smaller $\gamma(f)$, the easier it is to prove an asymptotic characterization result for f. In Section 3 we investigate $\gamma(f)$ and the existence of $n(f)$. With this in mind we partition the set $\mathscr{C}$ of polynomials in $\mathbb{Z}[x]$ in four disjoint sets: $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_{2,1} \cup \mathscr{C}_{2,2} \cup \mathscr{C}_3$. The set $\mathscr{C}_1$ contains the f for which K_f contains infinitely many primes. The set $\mathscr{C}_{2,1}$ contains the f not in $\mathscr{C}_1$ for which K_f contains exactly one prime p such that p^n is in K_f for every $n \geq 1$, and the set $\mathscr{C}_{2,2}$ contains the f not in $\mathscr{C}_1$ for which K_f contains at least two such primes. Finally the set $\mathscr{C}_3$ contains those f for which K_f is finite. Notice that the polynomials that are not in $\mathscr{C}_3$ inject $\mathbb{Z}$ into itself, so characterizing $D_f(n)$ for these f is non-trivial in the sense that $D_f(n)$ assumes infinitely many values. Furthermore $\mathscr{C}_1$, $\mathscr{C}_{2,1}$, $\mathscr{C}_{2,2}$, and $\mathscr{C}_3$ are disjoint and K_f is infinite if and only if f is in $\mathscr{C}_1 \cup \mathscr{C}_{2,1} \cup \mathscr{C}_{2,2}$. By the following well-known lemma (essentially on lifting of congruences), the condition that f is a permutation polynomial modulo p^n for every $n \geq 1$ is equivalent to the condition that f is a permutation polynomial modulo p^2.

LEMMA 2 [7, Corollary 4.3]. *Suppose f permutes $\mathbb{Z}/p\mathbb{Z}$. If the congruence*

$f'(x) \equiv 0 \pmod p$ does not have a solution, then f permutes $\mathbb{Z}/p^n\mathbb{Z}$ for every $n \geq 1$, otherwise f permutes $\mathbb{Z}/p^n\mathbb{Z}$ for $n = 1$ only.

We will show that Theorem 3 works (i.e., that $n(f)$ exists) for all f in $\mathscr{C}_1$, $\mathscr{C}_{2,2}$ and for a non-empty subset of $\mathscr{C}_{2,1}$. In particular, since cyclic polynomials of odd degree and Dickson polynomials of degree coprime to 6 are in $\mathscr{C}_1$, variants of Theorems 1 and 2 follow from Theorem 3 (cf. Examples 1 and 2). It is not difficult to show that $\mathscr{C}_{2,2}$ has a subset having positive density in the set $\mathscr{C}$ and that $\mathscr{C}_1$ has density zero (cf. Section 4). Thus Theorem 3 extends greatly the set of polynomials f for which $D_f(n)$ can be asymptotically characterized.

So far we have focused on characterizing discriminators. There is more to discriminators, however. Notice that $D_{f(g)}(n) \geq D_g(n)$ ($f(g)$ denotes $f(g(x))$, the composition of f and g). In particular it follows that $D(jk, n) \geq D(j, n)$ for arbitrary natural numbers j, k, and n. So $D(j, n)$ respects the multiplicative ordering of $\mathbb{N}$ in the first variable and the additive ordering in the second variable. Not surprisingly the behavior of $D(j, n)$ for fixed j is quite different from that for fixed n. For the latter see [9, 11]. To give an example from [9], using the technique that allowed Adleman, Fouvry and Heath-Brown to establish the first case of Fermat's Last Theorem for infinitely many prime exponents it can be shown that $D(j, n) = O((\log j)^{9/4})$. For Dickson polynomials there is a result analogous to $D(jk, n) \geq D(j, n)$. Put $G(j, n) = D_{g_j(x,1)}(n)$. Then using that $g_{kj}(x, 1) = g_k(g_j(x, 1), 1)$ one finds that $G(jk, n) \geq G(j, n)$.

2. Proof of Theorem 3

In this section we give the proof of Theorem 3.

Proof of Theorem 3. Assume that $n \geq n(f)$. By assumption there is at least one integer k in $[n, n/C(f)]$ such that f is a permutation polynomial modulo k. Let m be the smallest of these. Then $f(1), \ldots, f(m)$ are pairwise distinct modulo m and so are $f(1), \ldots, (n) = f(n)$; that is, $D_f(n) \leq m$. Since $m \in [n, n/C(f)]$ we have $n \geq C(f)m$. Put $r = D_f(n)$. Using the pigeonhole principle we find that $n \leq r \leq m$. We have to show that $r = m$. So assume that $n \leq r < m$. Then f cannot be a permutation polynomial modulo r. We have $V_f(r) \geq n \geq C(f)m > C(f)r$. Let ρ denote the squarefree part of r. Since for an arbitrary prime q and $h \geq 1$, $V_f(q^h) \leq q^{h-1}V_f(q)$, it follows that $(r/\rho)V_f(\rho) \geq V_f(r) > C(f)(r/\rho)\rho$ and so $V_f(\rho) > C(f)\rho$. By the Chinese Remainder Theorem $V_f(g) \leq C(f)g$ for all squarefree positive integers g such that f does not permute $\mathbb{Z}/g\mathbb{Z}$. It follows that f permutes $\mathbb{Z}/\rho\mathbb{Z}$, and since f does not permute $\mathbb{Z}/r\mathbb{Z}$, there must be a prime power p^e dividing r such that f permutes $\mathbb{Z}/p\mathbb{Z}$, but not $\mathbb{Z}/p^e\mathbb{Z}$. From this and Lemma

2 the existence of $1 \le x_0 \le p$ with $f'(x_0) \equiv 0 \pmod p$ follows. For every integer v we have $f(x_0 + vp^{e-1}) \equiv f(x_0) + vf'(x_0)p^{e-1} \equiv f(x_0) \pmod{p^e}$. Using the Chinese Remainder Theorem it follows from this that $f(x_0) \equiv f(x_0 + r/p) \pmod r$. In case $p = 2$ we have $x_0 + r/p \le 2 + r/2 < 2 + 3n/4 \le n + 1$, since $r < m \le n/C(f) \le 3n/2$ and $n \ge n(f) \ge 4$. Otherwise we have $x_0 + r/p \le p + r/p \le 2r/p < 3n/p \le n$. Since $1 \le x_0 < x_0 + r/p \le n$ and $f(x_0) \equiv f(x_0 + r/p) \pmod r$, we have a contradiction with the definition of r. It follows that $r = m$ and this proves the result. ∎

3. The Existence of $n(f)$

In this section we work out the form Theorem 3 takes for polynomials in the sets $\mathscr{C}_1$, $\mathscr{C}_{2,2}$, and $\mathscr{C}_{2,1}$ (note that Theorem 3 does not apply for f in $\mathscr{C}_3$). First we make a preliminary remark on the existence of $n(f)$.

Proposition 1. *Let d denote the degree of f. Suppose that $n_{(2d/(2d-1))}$ exists; then $n(f)$ exists.*

Proof. Suppose that $C(f) \le c < 1$ and that $n_{1/c}$ exists. Then $n(f) = n_{1/C(f)} \le n_{1/c}$ and so $n(f)$ exists. Since by Lemma 1, $C(f) \le 1 - 1/(2d) < 1$, the proposition follows. ∎

The following proposition facilitates the estimation of $C(f)$ $(= \max\{\frac{2}{3}, S(f)\})$ and $S(f)$.

Proposition 2. *Suppose that there exists a prime p satisfying*

$$\max\left\{\frac{V_f(q)}{q} \;\middle|\; V_f(q) < q, q \text{ prime}, q \le p\right\} \le \frac{dp - p + 1}{dp}. \tag{1}$$

Then $S(f) \le (dp - p + 1)/dp$. Furthermore if equality holds in (1), *then $S(f) = (dp - p + 1)/dp$.*

Proof. By Lemma 1, $V_f(q) \le [q - (q - 1)/d] \le q - (q - 1)/d$ and so $V_f(q)/q \le (dq - q + 1)/dq$ provided that $V_f(q) < q$. Since $(dq - q + 1)/dq$ is monotonic decreasing in q, the assumption (1) implies $\sup\{V_f(q)/q \mid V_f(q) < q, q > p\} < (dp - p + 1)/dp$ and so $S(f) \le (dp - p + 1)/dp$. The last part of the assertion is obvious now. ∎

3.1. *The Set $\mathscr{C}_1$*

The set $\mathscr{C}_1$ is very well understood. Schur conjectured (but see [17]), and Fried [6] proved (but see [16]), that up to linear translations, every polynomial that permutes $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p, i.e., every

polynomial in $\mathscr{C}_1$, can be written as the composition of cyclic and Dickson polynomials. For a polynomial f in $\mathscr{C}_1$ for which one knows a decomposition in terms of cyclic and Dickson polynomials, the integers k such that f permutes $\mathbb{Z}/k\mathbb{Z}$ can be determined using the following lemma.

LEMMA 3 [10, Lemma 11(iii)]. *For $j > 1$, $g_j(x, a)$ permutes $\mathbb{Z}/k\mathbb{Z}$ if and only if $(j, \psi_a(k)) = 1$ and the a-part of k is squarefree.*

Furthermore Lemma 3 allows one to conclude that f permutes $\mathbb{Z}/p\mathbb{Z}$ for all primes $p \equiv 2 \pmod{d}$ that are sufficiently large, where d is the degree of f. Using the Prime Number Theorem for arithmetic progressions it follows that n_μ exists for every $\mu > 1$, and by Proposition 1 so does $n(f)$. Thus we arrive at

THEOREM 3 ($\mathscr{C}_1$). *Suppose that f is in $\mathscr{C}_1$. Then $n(f)$ exists and, for every $n \geq n(f)$,*

$$D_f(n) = \min\{k \geq n \mid f \text{ permutes } \mathbb{Z}/k\mathbb{Z}\}.$$

EXAMPLE 1. Consider $f(x) = x^j$ for odd $j > 1$. It is an easy exercise to show that $V_f(p) = (p-1)/(j, p-1) + 1$. Since $V_f(p) = p$ for $p \equiv 2 \pmod{j}$, f is in $\mathscr{C}_1$. Using that f permutes $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/5\mathbb{Z}$, one finds that $S(f) \leq \frac{3}{7}$ and $C(f) = \frac{2}{3}$. It is easy to check that $D(j, n) = M_f(n)$ for $1 \leq n \leq 3$ and so the condition $n(f) \geq 4$ can be dropped. Using Theorem 3 ($\mathscr{C}_1$) and Lemma 3, one finds Theorem 1 with $4n/3$ replaced by $(3n + 1)/2$ (which sharpens Theorem 1).

EXAMPLE 2. Consider $f(x) = g_j(x, a)$, $a \neq 0$, $j \geq 5$ odd and not divisible by 3. Using a precise result for $V_{g_j(x,a)}$ [7, Theorem 3.27] one finds $S(f) \leq \frac{7}{11}$ and $C(f) = \frac{2}{3}$. As in Example 1 it can easily be seen that the condition $n(f) \geq 4$ can be dropped. On applying Theorem 3 ($\mathscr{C}_1$), Lemma 3, and the previous example, Theorem 2 with $2n - 3$ replaced by $3n/2$ results (which is weaker).

Notice that n_μ exists for every $\mu > 1$ if and only if $\gamma(f) = 1$. So for f in $\mathscr{C}_1$ we have $\gamma(f) = 1$.

3.2. *The Set $\mathscr{C}_{2,2}$*

For polynomials in this set Theorem 3 takes the following form.

THEOREM 3 ($\mathscr{C}_{2,2}$). *Let f be a polynomial in $\mathscr{C}_{2,2}$. Let $p_1, \ldots, p_s$ ($s \geq 2$) denote the primes such that f permutes $\mathbb{Z}/p_i^2\mathbb{Z}$ and $q_1, \ldots, q_t$ denote the primes such that f permutes $\mathbb{Z}/q_i\mathbb{Z}$, but not $\mathbb{Z}/q_i^2\mathbb{Z}$. Then $n(f)$ exists and, for every $n \geq n(f)$,*

$$D_f(n) = \min\{k \geq n \mid k = p_1^{\alpha_1} \cdots p_s^{\alpha_s} q_1^{\beta_1} \cdots q_t^{\beta_t}, \\ (\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) \in \mathbb{Z}_{\geq 0}^{t+s}, \beta_i \leq 1, i = 1, \ldots, t\}.$$

To prove this, we need the following result, the proof of which depends on some of the most elementary properties of continued fractions.

LEMMA 4. *Let $S = \{p_1, \ldots, p_s\}$ be a finite set of primes with $s \geq 2$. Then for any given $\mu > 1$ there exists an integer n_μ such that for every $n \geq n_\mu$ the interval $[n, \mu n]$ contains at least one integer having all its prime divisors in S.*

Proof. It suffices to prove the assertion with $S = \{p, q\}$ and $p < q$, p and q primes. Put $\alpha = \log p/\log q$. Notice that α is irrational (otherwise it follows that $p^a = q^b$ for some $a, b \geq 1$, which is impossible by the Fundamental Theorem of Arithmetic). Let r_n/s_n denote the nth convergent of the continued fraction expansion of α. Since α is irrational, r_n and s_n tend to infinity with n and we can choose n so large that $q^{1/s_n} \leq \mu$. Since, as is well known, $\alpha - r_n/s_n$ alternates sign, we can choose in addition n to be such that $\alpha - r_n/s_n$ is positive. Using that for convergents of irrational numbers one has $0 < |\alpha - r_k/s_k| < 1/s_k^2$ $(k \geq 1)$, we see that $1 < p^{s_n}/q^{r_n} < q^{1/s_n} \leq \mu$ and $1 < q^{r_{n+1}}/p^{s_{n+1}} < q^{1/s_{n+1}} \leq q^{1/s_n} \leq \mu$. In order to prove the assertion it is enough to construct a sequence of integers $\{n_i\}_{i=1}^{\infty}$ with $n_i < n_{i+1} \leq \mu n_i$ and n_i of the form $p^{a_i}q^{b_i}$ with $a_i, b_i \geq 0$. Put $n_1 = p^{s_{n+1}}q^{r_n}$. For any integer of the form p^aq^b not less than n_1 we must have $a \geq s_{n+1}$ or $b \geq r_n$. Write $n_i = p^{a_i}q^{b_i}$ for $i \geq 1$, and put $n_{i+1} = p^{a_i - s_{n+1}}q^{b_i + r_{n+1}}$ whenever $a_i \geq s_{n+1}$ and $n_{i+1} = p^{a_i + s_n}q^{b_i - r_n}$ otherwise. Since $n_i < n_{i+1} \leq \mu n_i$ and n_i is an integer for every $i \geq 1$, the assertion is established. ∎

Remark. Using Baker-type results on linear forms of logarithms one can prove much more, see, e.g., [15].

COROLLARY. *For f in $\mathscr{C}_{2,2}$ we have $\gamma(f) = 1$.*

Lemma 4 shows that n_μ $(\mu > 1)$ exists for f in $\mathscr{C}_{2,2}$. Thus, by Proposition 1, $n(f)$ exists and so Theorem 3 $(\mathscr{C}_{2,2})$ immediately follows from Theorem 3.

EXAMPLE 3. Put $f(x) = x^5 + x^3 - x$. Using Table 7.1 of [8] it is readily determined that 2, 3, and 5 are the only primes p such that f permutes $\mathbb{Z}/p\mathbb{Z}$. Furthermore, f permutes $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, and $\mathbb{Z}/25\mathbb{Z}$. Application of Proposition 2 with $p = 7$ yields $C(f) \leq \frac{29}{35}$. Consider the sequence $\{n_i\}_{i=0}^{\infty}$ with $n_{5k} = 2^{4+k} \cdot 3$, $n_{1+5k} = 2^{1+k} \cdot 3^3$, $n_{2+5k} = 2^{6+k}$, $n_{3+5k} = 2^{3+k} \cdot 3^2$, and $n_{4+5k} = 2^k \cdot 3^4$ $(k \geq 0)$. Since $n_{i+1} < \frac{35}{29} n_i$ for $i \geq 0$, we conclude that $n(f) \leq n_0 = 48$. By Theorem 3 $(\mathscr{C}_{2,2})$ it follows that for $n \geq 48$, $D_f(n) = \min\{k \geq n \mid k = 2^\alpha \cdot 3^\beta \cdot 5^\gamma\}$. In fact some further computation shows that this result already holds for $n \geq 1$.

3.3. *The Set $\mathscr{C}_{2,1}$*

The polynomials in this set have enough "permutational power" to ensure that there are infinitely many k for which f permutes $\mathbb{Z}/k\mathbb{Z}$, but not enough to make life easy; we shall show that this set contains polynomials for which

$n(f)$ exists and polynomials for which $n(f)$ does not exist. The criterion to decide which case applies is seen to depend on $C(f)$ and $\gamma(f)$. For f in $\mathscr{C}_{2,1}$ the latter quantity is computed most easily by the help of a certain directed graph. The structure of the graph depends only on certain numbers coming from f and so can be introduced in a polynomial-independent way.

Let $q \geq 2$ and $D \geq 1$ be arbitrary positive integers and $\mu > 1$ any real number. Based on these data only we construct a directed graph G_μ. To each positive divisor d of D we associate a vertex V_d. We draw a directed edge from a vertex V_{d_1} to a vertex V_{d_2} if and only if $w := \min\{q^n d_2/d_1 \mid n \in \mathbb{Z}, q^n d_2/d_1 > 1\} \leq \mu$. The number w is defined to be the *weight* of the directed edge. We do not require d_1 to be distinct from d_2. Notice that the number of vertices of G_μ is equal to the number of positive divisors of D. In case $\mu \geq q$ all edges do occur. There are no edges when μ is smaller than the smallest weight in G_q. The *weight of a path* is defined as the largest weight of the edges in the path.

LEMMA 5. *Let $q \geq 2$ and $D \geq 1$ be integers and $\mu > 1$ be a real number. There exists n_μ such that for every $n \geq n_\mu$ the interval $[n, \mu n]$ contains a number m of the form $m = q^\alpha d$, where d is a divisor of D, α is a non-negative integer, if and only if the graph G_μ contains a closed path.*

Proof. $\Rightarrow$ The assumption implies the existence of a sequence $\{n_i\}_{i=1}^\infty$ with $n_i < n_{i+1} \leq \mu n_i$ and $n_i = q^{\alpha_i} d_i$, where d_i divides D. Using our definition of weight, it follows that in G_μ the edges V_{d_i} and $V_{d_{i+1}}$ are connected by a directed edge. Thus the sequence $\{n_i\}_{i=1}^\infty$ corresponds with a path in G_μ. Since G_μ has only finitely many vertices, there has to be a closed path in G_μ.

$\Leftarrow$ By assumption G_μ contains a closed path. Let $V_{d_1}, \ldots, V_{d_s}$ denote the vertices on this path and $w_1, \ldots, w_s$ the weights corresponding to these vertices. We extend the closed path to an infinite path by extending it by itself infinitely often, e.g., $V_{d_1} = V_{d_{1+s}} = V_{d_{1+2s}} = \cdots$. It suffices to construct an infinite sequence $\{n_i\}_{i=1}^\infty$ of integers n_i satisfying $n_{i+1} \leq \mu n_i$, $n_{i+1} > n_i$ with n_i of the form $q^{\alpha_i} d_i$, where d_i divides D. To each vertex V_{d_j} in the path, we will construct a number n_j; we put $n_j = q^N d_1 \prod_{i=1}^j w_i$, where N for the moment is an arbitrary integer. Notice that

$$d_1 \prod_{i=1}^j w_i = d_{j+1} q^{\alpha_j}, \tag{2}$$

with $\alpha_j \in \mathbb{Z}$. Thus, we can choose N so large that n_j is an integer for $j = 1, \ldots, s-1$. Fix such a value of N. On choosing $j = s$ in (2) we see that $\prod_{i=1}^j w_i$ is a power of q. Since all weights exceed 1, $\prod_{i=1}^s w_i = q^\nu$ for some $\nu > 0$. It follows that n_j is an integer for every $j \geq 1$. Furthermore $n_{j+1} > n_j$ and $n_{j+1} = w_{j+1} n_j \leq \mu n_j$. Thus our sequence has all the required properties. ∎

DEFINITION. Let $\mu(q, D)$ be the smallest μ for which G_μ contains a closed path.

Using that G_q contains a closed path (e.g., the edge connecting V_1 with itself), we conclude that $\mu(q, D)$ exists. Notice that if D_1 divides D_2, then $\mu(q, D_2) \le \mu(q, D_1)$. By Lemma 5, $\mu(q, D)$ is the smallest μ such that there exists n_μ such that for every $n \ge n_\mu$ the interval $[n, \mu n]$ contains a number of the form $m = q^\alpha d$, where d divides D. Since the product of the weights in a closed path is at least q, the number of vertices s in a closed path in $G_{\mu(q,D)}$ satisfies $s \ge \log q/\log \mu(q, D)$. This shows that D must have many divisors in order for $\mu(q, D)$ to be close to 1. The following result, first proved by Zieve, shows that $\liminf_{D\to\infty} \mu(q, D) = 1$.

PROPOSITION 3. *Let a, d, and q be natural numbers with $a > q$ and α and d coprime. For every $\delta > 0$ there exist s and primes $q_1, \ldots, q_s$ in a, $a + d$, $a + 2d$, . . . such that $\mu(q, q_1 \cdots q_s) \le 1 + \delta$.*

Proof. Let $\{p_i\}_{i=0}^{\infty}$ be the sequence of consecutive primes in a, $a + d$, $a + 2d$, ... Let n_0 be such that $p_0 < q^{n_0+1}$. For $n \ge n_0$ put $p_{i_n} = \min\{p_r \mid p_r > q^n\}$ and $p_{j_n} = \max\{p_r \mid p_r < q^{n+1}\}$. Using the Prime Number Theorem for arithmetic progressions it follows that $\lim_{i\to\infty} p_{i+1}/p_i = 1$, so there exists n such that $p_i/p_{i-1} \le 1 + \delta$ for $i = i_n, \ldots, j_n + 1$. Put $q_0 = q^n$, $q_1 = p_{i_n}$, $q_2 = p_{1+i_n}$, . . . , $q_s = p_{j_n}$ and $m_{b+r(s+1)} = q^r q_b$ for $0 \le b \le s$, $r \ge 0$. Notice that $1 < m_{i+1}/m_i \le 1 + \delta$ for every $i \ge 1$. Thus $\mu(q, q_1 \cdots q_s) \le 1 + \delta$. ∎

EXAMPLE 4. Take $q = 2$ and $D = 3 \cdot 13$. Then $\mu(2, 39) = \frac{16}{13}$. The shortest closed path, $1 \to 39 \to 3 \to 13 \to 1$, is unique. The weights for this path are $\frac{39}{32}$, $\frac{16}{13}$, $\frac{13}{12}$, $\frac{16}{13}$, respectively.

We are now in a position to prove

THEOREM 3 ($\mathscr{C}_{2,1}$). *Let f be a polynomial in $\mathscr{C}_{2,1}$. Let p be the unique prime such that f permutes $\mathbb{Z}/p^2\mathbb{Z}$ and let $q_1, \ldots, q_t$ be the primes different from p such that f permutes $\mathbb{Z}/q_i\mathbb{Z}$. Suppose that $C(f)\mu(p, q_1 \cdots q_t) \le 1$. Then $n(f)$ exists and for every $n \ge n(f)$*

$$D_f(n) = \min\{k \ge n \mid k = p^\alpha q_1^{\beta_1} \cdots q_t^{\beta_t}, (\alpha, \beta_1, \ldots, \beta_t) \in \mathbb{Z}_{\ge 0}^{t+1}, \beta_i \le 1, \; i = 1, \ldots, t\}.$$

If $C(f)\ \mu(p, q_1 \cdots q_t) > 1$, then $n(f)$ does not exist.

Proof. By the definition of $\mu(p, q_1 \cdots q_t)$ and Lemma 5 it follows that $n_{\mu(p,q_1\cdots q_t)}$ exists. Since by assumption $1/C(f) \ge \mu(p, q_1 \cdots q_t)$, $n(f) = n_{1/C(f)} \le n_{\mu(p,q_1\cdots q_t)}$. It follows that $n(f)$ exists. If $1/C(f) < \mu(p, q_1 \cdots q_t)$

then by Lemma 5 and the definition of $\mu(p, q_1 \cdots q_t)$ it follows that $n(f)$ does not exist. ■

The constant $\mu(p, q_1, \ldots, q_t)$ appearing above is none other than $\gamma(f)$:

PROPOSITION 4. *Let f be in $\mathscr{C}_{2,1}$. Let p be the unique prime such that f permutes $\mathbb{Z}/p^2\mathbb{Z}$ and let $q_1, \ldots, q_t$ be the primes different from p such that f permutes $\mathbb{Z}/q_i\mathbb{Z}$. Then $\gamma(f) = \mu(p, q_1 \cdots q_t)$. In particular $\gamma(f) > 1$.*

Proof. Put $D = q_1 \cdots q_t$. Since $k_{i+1} \leq \gamma(f)k_i$ for all i sufficiently large, $[n, \gamma(f)n]$ contains an element of K_f for every n sufficiently large. Thus, by Lemma 5, $G_{\gamma(f)}$ contains a closed path and hence $\gamma(f) \geq \mu(p, D)$. Since $G_{\mu(p,D)}$ contains a closed path, it follows by Lemma 5 again that $k_{i+1} \leq \mu(p, D)(k_i + 1)$ for i sufficiently large; that is, $\gamma(f) \leq \mu(p, D)$. Since $\mu(p, D)$ equals the weight of some edge in G_q and a weight always exceeds one, the final part of the assertion follows. ■

EXAMPLE 5. Consider $f(x) = x^5 + 117x^3 + 78x^2 + 39x$. Using Table 7.1 of [8] one concludes that 2, 3, and 13 are the only primes p such that f permutes $\mathbb{Z}/p\mathbb{Z}$. Moreover, f permutes $\mathbb{Z}/4\mathbb{Z}$, but permutes neither $\mathbb{Z}/9\mathbb{Z}$ nor $\mathbb{Z}/169\mathbb{Z}$. Application of Proposition 2 with $p = 31$ yields $C(f) \leq \frac{25}{31}$. By Example 4, $\mu(2, 39) = \frac{16}{13}$, so $\mu(2, 39)C(f) \leq \frac{400}{403} < 1$ and thus f satisfies the condition of Theorem 3 ($\mathscr{C}_{2,1}$). Using the sequence $\{n_i\}_{i=0}^{\infty}$ defined by $n_{4k} = 2^{5+k}$, $n_{1+4k} = 2^k \cdot 3 \cdot 13$, $n_{2+4k} = 2^{4+k} \cdot 3$, $n_{3+4k} = 2^{2+k} \cdot 13$ ($k \geq 0$), one finds $n(f) \leq 32$. So $\mu(2, 39)C(f) \leq \frac{400}{403} < 1$ and thus $D_f(n) = \min\{k \geq n \mid k = 2^a d, d \mid 39\}$, for every $n \geq 32$. This result even holds for $n \geq 1$.

EXAMPLE 6. Consider $f(x) = x^5 + 3x^3 + 3x$. Using Table 7.1 of [8] one concludes that 2 and 3 are the only primes p such that f permutes $\mathbb{Z}/p\mathbb{Z}$. Moreover, f permutes $\mathbb{Z}/4\mathbb{Z}$, but does not permute $\mathbb{Z}/9\mathbb{Z}$ and so is in $\mathscr{C}_{2,1}$. Since $V_f(29) = 23$, $C(f) \geq \frac{23}{29}$. Since $\mu(2, 3)C(f) \geq \frac{69}{58} > 1$, f does not satisfy the condition of Theorem 3 ($\mathscr{C}_{2,1}$) and moreover the number $n(f)$ does not exist.

If $d \geq 3$, $f \in C_{2,1}$, $\gamma(f) < d/(d-1)$, and $\gamma(f)C(f) > 1$, there exists $a \in \mathbb{Z}$ such that $a \cdot f \in C_{2,1}$ and $\gamma(a \cdot f)C(a \cdot f) \leq 1$, and hence a characterization for $D_{a \cdot f}(n)$ as given by Theorem 3 ($C_{2,1}$) holds, whereas Theorem 3 ($C_{2,1}$) does not guarantee the existence of such a characterization for $D_f(n)$. Let q be a prime so large that $1/\gamma(f) \geq (dq - q + 1)/(dq)$. Take $a = \prod_{r \leq q, r \notin K_f} r$, with r prime. Then $a \cdot f \in C_{2,1}$. Furthermore $C(a \cdot f) \leq (dq - q + 1)/(dq)$ and $\gamma(a \cdot f)C(a \cdot f) = \gamma(f)C(a \cdot f) \leq 1$.

Although for the polynomial of Example 6, $n(f)$ does not exist, computation suggests that for all $n \geq 1$, a characterization as given by Theorem 3 is valid. Thus it seems that the sufficient criterion $C(f)\mu \leq 1$ for the existence of an asymptotic characterization as given by Theorem 3 ($\mathscr{C}_{2,1}$) is not necessary. Obviously a necessary condition for the existence of such a character-

ization is that f permutes $\mathbb{Z}/k\mathbb{Z}$ for infinitely many k. The next example shows that this condition is not sufficient.

EXAMPLE 7. (Zieve [20]). Put $f(x) = 5x^3 - 2x$. Using Table 7.1 of [8] one concludes that f permutes $\mathbb{Z}/k\mathbb{Z}$ if and only if k is a power of 5 or twice a power of 5. So $f(a) \equiv f(b) \pmod{5^m}$ yields $a \equiv b \pmod{5^m}$; furthermore $f(a) \equiv f(b) \pmod 4$ yields that a and b must be both even or $a \equiv b \pmod 4$. Put $n = 1 + 2 \cdot 5^m$. It follows that $f(1), f(2), \ldots, f(n)$ are distinct modulo $4 \cdot 5^m$. But $2 \cdot 5^m < n < 4 \cdot 5^m < 5^{m+1}$, so $D_f(n)$ cannot be a power of 5 or twice a power of 5. Since m is arbitrary, an asymptotic characterization as given by Theorem 3 ($\mathscr{C}_{2,1}$) cannot exist.

EXAMPLE 8. Along the lines of Example 7, Zieve showed in [21] that the discriminator of the polynomial $f(x) = 3px^3 - 6q_1 \cdots q_t x$, where the q_i are odd satisfying $q_i \equiv 2 \pmod 3$ for $1 \le i \le t$ and $q_1 \cdots q_t < p$, does not have an asymptotic characterization as given by Theorem 3 ($\mathscr{C}_{2,1}$). Drop the condition $p > q_1 \cdots q_t$ and assume $p \ge 5$. By Proposition 3 there exist s and primes $q_i > p$ satisfying $q_i \equiv 2 \pmod 3$ for $1 \le i \le s$ such that $\mu(p, 2q_1 \cdots q_s) \le \frac{15}{11}$. Then $C(f)\gamma(f) = C(f)\mu(p, 2q_1 \cdots q_s) \le 1$ and so an asymptotic characterization as given by Theorem 3 ($\mathscr{C}_{2,1}$) exists.

Example 8 shows there are polynomials of degree 3 in $\mathscr{C}_{2,1}$ with asymptotic characterization. Working a little bit harder we can show there are polynomials with this property of arbitrary degree ≥ 2 in this set. In order to show this we use the following two results, the first of which is due to Cohen [4] and answers a conjecture of Chowla and Zassenhaus dating from 1968.

LEMMA 6. *Let $f \in \mathbb{Z}[x]$ be of degree $d \ge 2$. Then for any prime $p > (d^2 - 3d + 4)^2$ for which f permutes $\mathbb{Z}/p\mathbb{Z}$ and p does not divide the leading coefficient of f, there is no integer $1 \le c < p$ for which $f(x) + cx$ also permutes $\mathbb{Z}/p\mathbb{Z}$.*

LEMMA 7. *Let f be of degree $d \ge 2$ and c a non-zero integer. Then not both $f(x)$ and $f(x) + cx$ can permute $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p.*

Proof. Suppose that both $f(x)$ and $f(x) + cx$ permute $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p. Then both of them are compositions of Dickson polynomials (of degree not divisible by 3) and cyclic polynomials of odd degree. Using Lemma 3 we conclude that both will permute $\mathbb{Z}/p\mathbb{Z}$ for all primes $p \equiv 2 \pmod d$ that are sufficiently large. Let $p > \max\{(d^2 - 3d + 4)^2, |c|\}$ be such a prime. Then Lemma 6 yields a contradiction. ∎

LEMMA 8. *Let $d \ge 2$. There exist polynomials of degree d in $\mathscr{C}_{2,1}$ that have an asymptotic characterization as given by Theorem 3 ($\mathscr{C}_{2,1}$).*

Proof. Put $f = 89x^2 + 2x$. Notice that $C(f)\gamma(f) = C(f)\mu(89, 2) = \frac{256}{267}$. The case $d = 3$ has been dealt with in Example 8, so we may take $d \ge 4$.

By Proposition 3 there exist s and primes $q_i > p$ satisfying $q_i \equiv 2 \pmod 3$ for $1 \le i \le s$ such that $\mu(p, 2q_1 \cdots q_s) \le 2d/(2d-1)$. Consider $f_1(x) = pq_1 \cdots q_s x^d + px^3 + q_1 \cdots q_s x$ and $f_2(x) = f_1(x) + q_1 \cdots q_s x$. Both f_1 and f_2 permute $\mathbb{Z}/q_i\mathbb{Z}$, but not $\mathbb{Z}/q_i^2\mathbb{Z}$, for $1 \le i \le s$ and $\mathbb{Z}/p^n\mathbb{Z}$ for every $n \ge 1$. By Lemma 7 we can pick one of f_1 and f_2, denote it by g, that is not a permutation polynomial for infinitely many primes. Thus the product of the primes q such that q^2 is in K_g and $q \ne p$ is finite. Denote it by a. Notice that $a \cdot g$ is in $\mathscr{C}_{2,1}$. Furthermore

$$C(a \cdot g)\gamma(a \cdot g) \le C(a \cdot g)\mu(p, q_1 \cdots q_s) \le C(a \cdot g)\frac{2d}{2d-1} \le 1,$$

where the latter inequality holds by Lemma 1. ■

4. Density Considerations

Given a set S of polynomials in $\mathbb{Z}[x]$ and an integer $n \ge 1$, we define the density $\delta_n(S)$ of S as

$$\delta_n(S) = \lim_{A \to \infty} \frac{|S_n(A)|}{|P_n(A)|},$$

where $P_n(A) = \{f \in \mathbb{Z}[x] \mid \deg f \le n$ and maximum coefficient size $\le A\}$ and $S_n(A) = S \cap P_n(A)$, provided that the limit exists. Put $S_p = \{f \in \mathbb{Z}[x] \mid f$ permutes $\mathbb{Z}/p^2\mathbb{Z}\}$ for a given prime p.

Proposition 5. *For $n \ge 2p-1$ one has*

$$\delta_n(S_p) = \frac{(p-1)!(p-1)^p}{p^{2p-1}} = e^{-(p+1)}\sqrt{2\pi p}\left(1 + O\left(\frac{1}{p}\right)\right).$$

Proof. This is an exercise in linear algebra that is left to the reader. The latter equality follows on applying Stirling's formula in the form $n! = n^n e^{-n}\sqrt{2\pi n}(1 + O(n^{-1}))$. ■

Proposition 6. *For $n \ge 1$, $\delta_n(\mathscr{C}_1) = 0$.*

Proof. Since a polynomial of even degree cannot be in $\mathscr{C}_1$ it follows that $\delta_n(\mathscr{C}_1) = 0$ for n even, so assume that n is odd. Let $A \ge 1$ be an integer. Let f be any polynomial in $\mathscr{C}_1$ of degree n (e.g., x^n) and let $q > \max\{(d^2 - 3d + 4)^2, 2A + 1\}$ be any prime such that f permutes $\mathbb{Z}/q\mathbb{Z}$. Using Lemma

6 it follows that there are at most $(2A + 1)^n$ polynomials in $\mathscr{C}_1 \cap P_n(A)$. So $0 \leq \delta_n(\mathscr{C}_1) \leq \lim_{A\to\infty}(2A + 1)^n/(2A + 1)^{n+1} = 0$. ■

Put $S'_p := \{f \in S_p \mid f \notin \mathscr{C}_1\}$. Proposition 6 implies that $\delta_n(S'_p) = \delta_n(S_p)$. Since any $g_j(x, 1)$ with $(j, p(p^2 - 1)) = 1$ is in $S_p \cap C_1$, we have $S'_p \neq S_p$. It is not true, however, that $\mathscr{C}_1$ is a subset of $\bigcup_p S_p$ (consider x^j with j odd). Notice that $\mathscr{C}_3$ equals the set theoretical complement of $\bigcup_p S'_p \cup C_1$ and that $\mathscr{C}_{2,2} = \bigcup_{p<r}(S'_p \cap S'_r)$, where the union is taken over all prime pairs (p, r) with $p < r$. Using the chinese remainder theorem and Proposition 6 one deduces, for $r \geq 1$, that $\delta_n(S'_{p_1} \cap \cdots \cap S'_{p_r}) = \delta_n(S_{p_1})\delta_n(S_{p_2}) \cdots \delta_n(S_{p_r})$, with $p_1, \ldots, p_r$ distinct primes. Using this and Proposition 6 it follows that for $n \geq 13$ the set $\mathscr{C}_3$ is contained in a set having density not exceeding 0.806 (the complement in $\mathbb{Z}[x]$ of $S'_2 \cup S'_3 \cup S'_5 \cup S'_7$ will do) and that $\mathscr{C}_{2,2}$ has a subset having density exceeding 0.01 (the set $(S'_2 \cap S'_3) \cup (S'_2 \cap S'_5) \cup (S'_3 \cap S'_5)$ will do). By considering other sets these two densities can be hardly decreased respectively increased. It thus seems reasonable to conjecture that $\delta_n(\mathscr{C}_{2,1})$, $\delta_n(\mathscr{C}_{2,2})$, and $\delta_n(\mathscr{C}_3)$ exist and that $\delta_n(\mathscr{C}_{2,1}) \approx 0.193$, $\delta_n(\mathscr{C}_{2,2}), \approx 0.01$, and $\delta_n(\mathscr{C}_3) \approx 0.806$ for all n large enough.

5. Conclusion

In case f is in $\mathscr{C}_1$ or $\mathscr{C}_{2,2}$ or in a non-empty subset of $\mathscr{C}_{2,1}$, there exists an asymptotic characterization of the form

$$D_f(n) = \min\{k \geq n \mid f \text{ permutes } \mathbb{Z}/k\mathbb{Z}\}.$$

Recall that $K_f = \{k \geq 1 \mid f \text{ permutes } \mathbb{Z}/k\mathbb{Z}\}$ and that $\gamma(f) = \limsup_{i\to\infty} k_{i+1}/k_i$, where $k_1, k_2, \ldots$ denote the consecutive elements of K_f. We have $\gamma(f) = 1$ if f is in $\mathscr{C}_1 \cup \mathscr{C}_{2,2}$ and $\gamma(f) > 1$ otherwise. In case f permutes $\mathbb{Z}/k\mathbb{Z}$ for only finitely many k, i.e., when f is in $\mathscr{C}_3$, a characterization as above is impossible. Characterizing $D_f(n)$ for these f remains completely open. The polynomials $g_j(x, a)$, $a \neq 0$, j odd, $3 \mid j$ belong to this set. Already a glance at the table in [10] gives the impression that in this case a characterization (if any exists) will have a very different form.

Acknowledgments

The author thanks Jilyana Cazaran, S. D. Cohen, M. Fried, H. W. Lenstra, Jr., R. Matthews, I. Shparlinski, P. Solé, D. Wan, K. S. Williams, the referees, and, especially, M. Zieve. The latter has, using a more algebraic geometric approach (he uses, e.g., Weil's bounds), improved on some of the results here and established further results [20]. This article was written while

the author was a postdoc at Macquarie University, whose support in terms of computer facilities and nice atmosphere is acknowledged.

REFERENCES

1. L. K. Arnold, S. J. Benkoski, and B. J. McCabe, The discriminator (a simple application of Bertrand's Postulate), *Amer. Math. Monthly* **92** (1985), 275–277.
2. M. Barcau, A sharp estimate of the discriminator, *Nieuw Arch. Wisk.* **6** (1988), 247–250.
3. P. S. Bremser, P. D. Schumer, and L. C. Washington, A note on the incongruence of consecutive integers to a fixed power, *J. Number Theory* **35** (1990), 105–108.
4. S. D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, *Canad. Math. Bull.* **33** (1990), 230–234.
5. H. Davenport, "Multiplicative Number Theory," 2nd ed., Springer-Verlag, New York, 1980.
6. M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970), 41–55.
7. R. Lidl, G. L. Mullen, and G. Turnwald, "Dickson Polynomials," Pitman Monographs in Pure and Applied Mathematics, Vol. 65, Longman Scientific, Essex, England, 1993.
8. R. Lidl and H. Niederreiter, "Finite Fields," Encyclo. Math. Appl., Vol. 20, Addison–Wesley, Reading, MA, 1983.
9. P. Moree, Discriminators and the first case of Fermat's Last Theorem, unpublished manuscript.
10. P. Moree and G. L. Mullen, Dickson polynomial discriminators, *J. Number Theory,* to appear.
11. P. Moree and H. Roskam, On an arithmetical function related to Euler's totient and the discriminator, *Fibonacci Quart.* **33** (1995), 332–340.
12. G. L. Mullen, Permutation polynomials over finite fields, *in* "Proceedings of the International Conference on Finite Fields, Coding theory and Advances in Communications and Computing," pp. 131–151, Lecture Notes in Pure and Appl. Math., Vol. 141, Dekker, New York, 1992.
13. P. Schumer, On the incongruence of consecutive cubes, *Math. Student* **58** (1990), 42–48.
14. P. Schumer and J. Steinig, On the incongruence of consecutive fourth powers, *Elem. Math.* **43** (1988), 145–149.
15. R. Tijdeman, On integers with many small prime factors, *Comp. Math.* **28** (1974), 159–162.
16. G. Turnwald, On a problem concerning permutation polynomials, *Trans. Amer. Math. Soc.* **302** (1987), 251–267.
17. G. Turnwald, On Schur's conjecture, *J. Austral. Math. Soc.* **58** (1995), 312–357.
18. G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* **1** (1995), 64–82.
19. D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, *in* "Proceedings of the International Conference on Finite Fields, Coding Theory and Advances in Communications and Computing," pp. 209–216, Lecture Notes in Pure and Appl. Math., Vol. 141, Dekker, New York, 1992.
20. M. Zieve, Note on the discriminator, I, unpublished manuscript, 1994.
21. M. Zieve, Note on the discriminator, II, unpublished manuscript, 1995.